DEFENSE MECHANISM OF SOPHISTICATED ATTACK USING ZKP-ECDH PROTOCOL IN WSN

[1]A Vijay, [2]M Suresh
[1]Assistant professor, Faculty of Engineering, Karpagam University
[2]Research scholar, Karpagam University

Abstract: In smart cities, wireless sensor network is affected because of ongoing attacks and unidentified attacks are sophisticated attacks that cause the WSN to function in abnormal behavior manner. In this paper, we propose a new defense framework to detect the sophisticated attack and authenticate the communication between nodes using authentication protocol. The proposed work can be analyzed using various performance metrics such as detection ratio, false detection ratio, packet delivery ratio, and average delay and control overheads. The experimental is performed using Ns-2 simulator tool and result proved that the proposed work outperforms well than existing work.

Keyword: sophisticated attack, wireless sensor network, ZKP-ECDH protocol, smart cities.

1. INTRODUCTION

A WSN consists of circulated self-governing sensors to monitor physical or environmental conditions [1].In most of the application scenarios, WSNs are expected to operate independently and in an unsupervised manner and hence the nodes are exposed to a variety of attacks. In smart cities, wireless sensor networks (WSNs) act as a type of core infrastructure that collects data from the city to implement smart services[2]-[5]. Providing security services in these networks and preventing from attacks are the most important challenges for these networks.

The security of WSNs is one of the key issues of smart cities [6]. Some attacks are actually sophisticated that means it possess a serious threat to the data. This type of attack can cross the limit of standard security measures such as firewalls, malware detection and intrusion detection systems. This attack possesses a severe hazard to the operations and safety of manufacturing companies. Existing defenses may work only against older threats, but it cannot prevent the newer and further sophisticated attacks. Characteristics of a 'sophisticated' attack are given below:

- The adversary recognized exactly what application they were wanted to cause the attack and gathered intelligence regarding their target.2. They utilized the collected intelligence to violent the particular points in their target, and not just a random system on the network.
- They avoided several layers of robust defense mechanisms such as include firewall, intrusion prevention systems, encryption, multi-factor authentication and so on.
- They attached multiple exploits to attain their full negotiation. During the attack, a zero-day has been utilized. There should be some clever or distinct method that was used.
- If malware was used in the attack, then it had to be malware that would not have been detectable using up-to-date anti-virus, payload recognition, or other endpoint security software.
- If an attack exhibits most or all of these characteristics, it can be considered 'sophisticated'.

2. RELATED WORKS

There are security mechanisms already in use in some existing applications such as VoIP enterprise environments, trust management, web services, and so on that were developed to address various types of attacks including ongoing and unknown attacks [7]–[9]. However, these schemes cannot be used directly in WSNs. Presently; two types of security methods exist to defend WSNs: detection-based methods and prevention-based method. Though many defense methods have been planned to address the intrusion detection and access control for WSNs [6],[10]-[14], these two types of approaches have traditionally been studied separately. In order to enhance the defense mechanism of WSNs, security framework is proposed in this paper that contains the attack detection and access control. The traditional prevention methods are used in WSNs [6][10]. But, the proposed framework is dissimilar to existing methods. The proposed method uses usage control (UCON) with endless decision making and dynamic attributes. These features are

supporting in defend against ongoing threats. The proposed work is dissimilar from most existing detection approaches [10]–[14].

3. PROPOSED METHODOLOGY

The proposed framework for detecting the attacks and providing security in wireless sensor network is divided into 4 modules.

- Usage control
- KeyGraph mechanism for known attacks
- Attack mitigation
- Authentication model

3.1 Usage control

Usage control (UCON) is a new type of prevention technology. UCON performs data control not only at the time of access but also during and after use. Continuous decisions with regard to data access can be made before the access is allowed, during a user's session, or even (via an event) after the session ends. Moreover, during use or after usage has been authorized, its attributes can be changed before access is approved. The defense level can be significantly improved by this continuous control. In addition to this, security capabilities have been used like data rights management (DRM).

3.2 Key Graph mechanism

Key Graph mechanism is used for detecting the known attacks. It mines key points from the information and then links the relations between points as an intuitionistic graph. The lines between the nodes defines relationships between data and quantify the volume of ``tightness" between the items. The feature nodes with values beyond a reasonable threshold are treated as detection rules that must be satisfied for attack detection; thus, a detection rule can be constructed.

3.3 Attack Mitigation using SDN and NFV

Based on the attack graph driven by evidence, the SDN controller inspects all the VNFs that have already been registered and determines an attack mitigation plan for the current situation that obeys a pre-defined security policy. The algorithms that determine the attack mitigation plan are discussed in next module. The SDN controller obtains the attack mitigation plan and installs the VNF instances into the selected network nodes. VNFs can be deployed as binary compiled code or as interpreted language scripts. When these steps are complete, the mobile network can defend against the threat.

Authentication model

Elliptic Curve Diffie Hellman (ECDH) protocol begins to share the key among two parties. The original Diffie-Hellman(DH) algorithm is depend on the multiplicative group modulo p, but ECDH protocol is depend on the additive elliptic curve group. All base point P(x, y) of order n is chosen on the elliptic curve E over the field GF (p) or (2) k GF.

SENDER SIDE	RECEIVER SIDE
i . $Select\ random\ number\ d_U \in [2, n-2]$	i . $Select\ random\ number\ d_s \in [2, n-2]$
ii . $Compute\ f_U = d^{-1}{}_U mod\ n\ and\ M_U = d_U K$	ii . $Compute\ f_S = d^{-1}{}_S mod\ n\ and\ M_U = d_U K$
iii . $Send\ M_U\ to\ Server\ S$	iii . $Receive\ M_U$
iv . $Receive\ E_S$	iv . $Compute\ E_S = d_S M_U = d_S d_U K$
v . $Compute\ S_U\ to\ the\ server\ S$	v . $Send\ E_S\ to\ User\ U$
	vi . $Receive\ S_U$
	vii $Compute\ T = f_S S_U = f_S d_S K = K$

Authentication protocol is proposed which is very helpful for group communication among big companies where shareholders are very busy and cannot attend all the meetings. Most of the authentication protocols based on ECC use the ECDSA. The reason behind this is that it provides a high level of security. For our proposed protocol we use the zero knowledge to authenticate the users. A zero Knowledge protocol is an interactive technique for one party to prove to another that a statement is true without revealing anything other than the veracity of the statement.

A zero knowledge protocol must satisfy three properties

(i) Completeness: It means that if the statement is true, the honest verifier (that is, one following the protocol property) will be convinced of this fact by an honest prover.

(ii)Soundness: It means that if statement is not true no cheating prover can convince the honest verifier that it is true, except with some small probability.

(iii) Zero Knowledge: It means that if the statement is true, no cheating verifier learns anything other than this fact.

The aim of the zero knowledge is to prove the knowledge of a secret without revealing it. Each user from the group has secret information and each one has to prove that he/she knows the information without revealing it to the server. Thus the prover is the user and the verifier is the server. Since the secret information of each user is different therefore the server will identify each user through a demonstration of his knowledge. The basic idea of the zero knowledge authentications is that the verifier asks a question related to the secret information in such a way that the answer does not reveal the secret. Schnorr's protocol is one of the most popular zero knowledge protocol.

Let p and q be two primes number such that q divides (p 1). Let g 1be an element of order q in p Z (the multiplicative group of integers modulo p). Also let q G be the cyclic subgroup of order q generated by g . The integers p,q, g are known and can be common to a group of users. An identity consists of a private /public key pair. The private key w is a random non-negative integer less than q

The public key is computed as

$$y = g^{-w} mod\ p$$

The protocol is described as below Common Input: p, q, g, y; security parameter t.

Secret Input for a Prover: $w \in Z_q$ such that

$$y = g^{-w} mod\ p$$

A) Commitment by Prover Prover picks, $r \in Z_q$

Compute $x = g^r mod\ p$ and s0065nd it to the verifier

$$Prover \overset{x=g^t}{} Verifier$$

B) Challenge from Verifier

Verifier selects a number $e \in [1\ 2^t]$ and sends it to the prover

$$Prover \overset{e}{} Verifier$$

C) Response from Prover:

Prover computes

$S = r + w.e\ modq$, and sends it to the verifier

$$Prover \overset{s=r+w.e}{} Verifier$$

The verifier checks that $x = g^s y^e mod\ p$ and accepts if and only if equality holds. It is well known that Schnorr's protocol is an honest verifier zero knowledge protocol of knowledge of, the discrete logarithm of y Schnorr's protocol based on elliptic curve is described as below .Let be a point on the elliptic curve defined over the finite field, of order (Prover's secret information key), then

- **(i)** If α is the prover's secret information then user makes public.$Z = \alpha P$
- **(ii)** The prover picks a random number r and sends $X = rP$ to the verifier
- **(iii)** The verifier picks a random number e and sends it to the prover.
- **(iv)** The prover computes

$Y = \alpha e + r \ mod n$, and sends it to the verifier.

(v) The receiver receives y and accept if

.

$$yP + eZ = X$$

Communication Process among the group once the verification procedure is completed by the sender and the receiver, the communication can start among the authenticated users of the group. All the users use the same key pair (P (public key), S (secret key)) because they all have to know the messages sent from any user of the group. This key pair along with the server's one is used for communication during each session. Two users cannot communicate through this protocol without the knowledge of the others. If one user receives a message it can be read by all the others because they all can decrypt it. Further if one user's key is found by an intruder all the users are affected. The security level can be increased by keeping a point P (private) on elliptic curve E. The public parameters are the prime number p and a, b defining the elliptic curve $E_P(a, b)$ such that $y^2 = x^3 + ax + b$ with $\gcd\ 4a^3 + 27b^2, p = 1$. The RSA algorithm is used to generate the key pair (e, d).

If A and B are two communicating parties then algorithms is described below

(i) A Selects two random numbers $X_A, R_A \ in \ E_P$ and a point P_A on elliptic curve.

(ii) B Selects two random numbers $X_B, R_B \ in \ E_P$ and a point P_B on elliptic curve.

(iii) A sends $G_A = X_A P_A \ to \ B$

.

(iv) B Sends $G_B = X_B P_B \ to \ A$

.

(v) A Sends $S_A = R_A G_B \ to \ B$

.

(vi) B Sends $S_B = R_B G_A \ to \ A$

(vii) A Computes the session key

$$Pub = e(S_A + S_B)$$

(viii) B computes the session key

$$Pub = d(S_A + S_B)$$

.

(ix) The private key will be

$$Sec = d(S_A + S_B)$$

4. EXPERIMENTAL RESULT

In the experimental analysis, the behavior of nodes in wireless sensor network and its performance are analyzed using proposed method. The proposed methodology is implemented using NS-2. It is popular and well known network simulator tool. This tool is used in the area of MANET, wireless sensor network, etc. In this work, the network consists of 50 mobiles nodes and 5 malicious nodes. The number of malicious nodes is varied with time. The analysis is made in the proposed work. The simulation parameters are used while implementing this proposed technique is summarized below in the Table1. These parameters are used to construct the network.

Table 4.1: Simulation Parameters

Simulation Parameters	Values
Propagation	TwoRayGround
Channel	WirelessChannel
Physical layer	WirelessPhysical
Queue	DropTail/PriQueue
Mac	802.11
X dimension of the topography	500
Y dimension of the topography	500
Adhoc routing	AODV
Antenna	Omni Antenna
Max packet	100
No of nodes simulated	50
Cp	./cbr
Sc	Nodes50
Simulation time	200s(Min: 200s, Max: 10000s)
Energy	EnergyModel
Initial Energy	100
Minimum Neighbor	6
No of Malicious nodes	5

4.2 Performance evaluation

The proposed methodology is simulated. Network Simulator is used to create the experimental setup. The performance of the proposed method is evaluated in terms of,

- Average Delay
- Packet Delivery Ratio
- Overhead
- False detection ratio
- Detection ratio and
- Packet loss

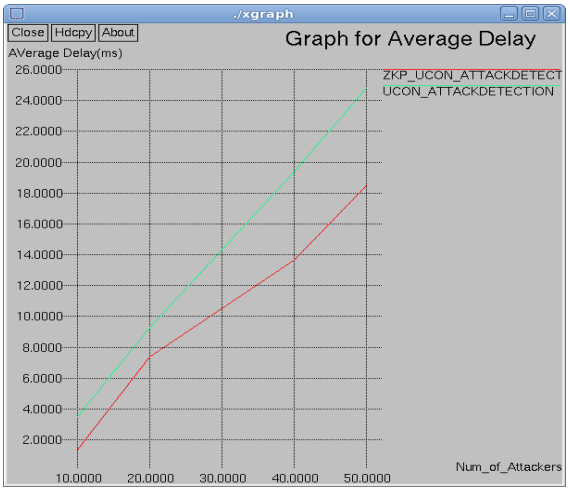

Figure 1: Average Delay

From Figure 4.1, the average delay of proposed methodology is lower than average delay of existing method UCON.

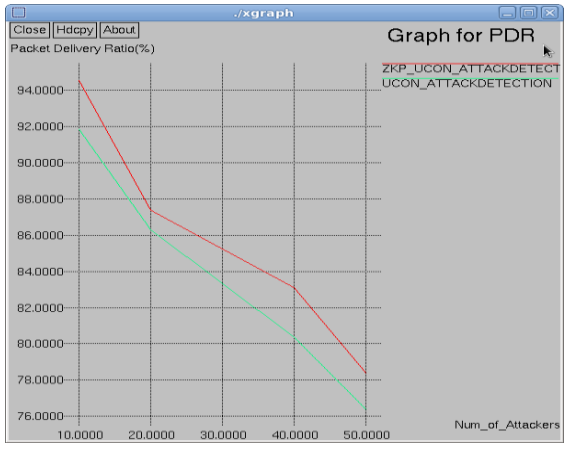

Figure 2: Packet delivery ratio

From Figure 4.2, the packet delivery ratio of proposed methodology is higher than packet delivery ratio of existing method UCON.

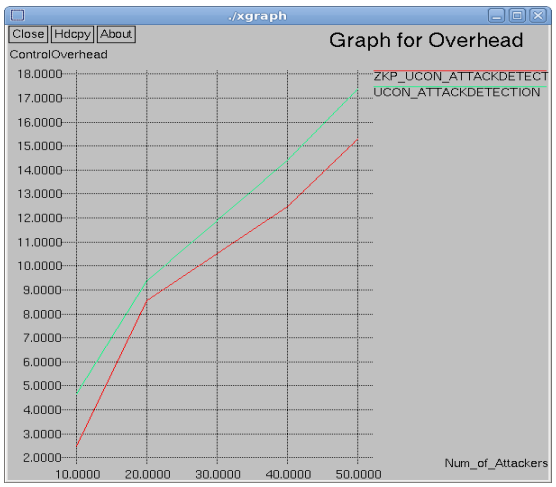

Figure 3: Overhead

From Figure 4.3, the packet overhead of proposed methodology is lower than overhead of existing method UCON.

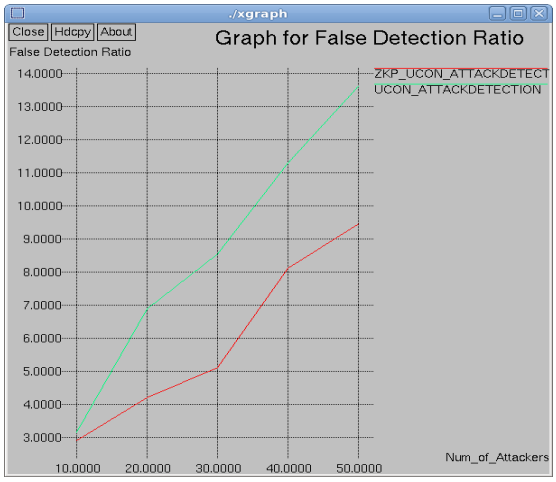

Figure 4: False detection ratio

From Figure 4.4, the false detection ratio of proposed methodology is lower than false detection ratio of existing method UCON.

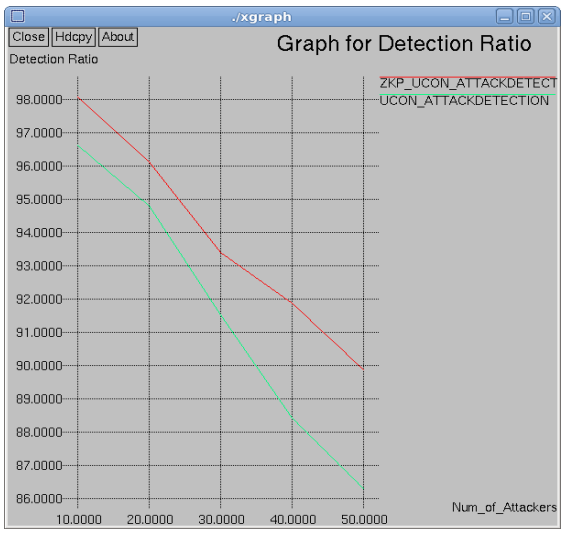

Figure 5: Detection ratio

From Figure 4.5, the detection ratio of proposed methodology is higher than detection ratio of existing method UCON.

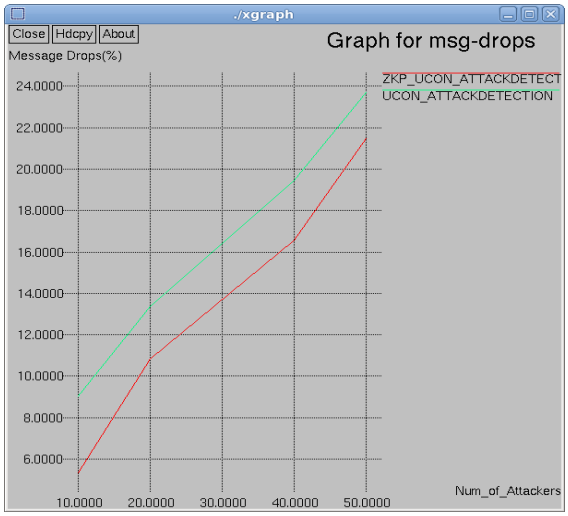

Figure 6: Message drop

From Figure 4.6, the Message drop of proposed methodology is lower than Message drop of existing method UCON.

5. CONCLUSION

Security of Mobile Wireless Sensor Networks is a vital challenge as the sensor nodes are deployed in unattended environment and they are prone to various attacks. One among them is sophisticated attack. The proposed defense framework is used to detect the sophisticated attack and authenticate the communication between nodes using authentication protocol. The experiment is conducted using the ns-2 simulator. The proposed method has less overhead, and low false alarm rate. The results of the proposed approach are compared with existing method which shows that the minimized the average delay, control overhead, and message drops and maximized the packet delivery ratio value and detection ratio.

REFERENCES

[1] Himani Chawla,"Some issues and challenges of Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, ISSN: 2277 128X, July 2014.

[2] K. Ota, M. Dong, J. Wang, S. Guo, Z. Cheng, and M. Guo, ''Dynamic itinerary planning for mobile agents with a content-specific approach in wireless sensor networks,'' in Proc. IEEE 72nd Veh. Technol. Conf.Fall (VTC-Fall), Ottawa, ON, Canada, Sep. 2010, pp. 1–5.

[3] S. Chang, Y. Qi, H. Zhu, M. Dong, and K. Ota, ''Maelstrom: Receiver-location preserving in wireless sensor networks,'' in Proc. 6th Int. Conf. Wireless Algorithms, Syst., Appl. (WASA), Chengdu, China, 2011,pp. 190–201.

[4] L. Guo, J. Wu, Z. Xia, and J. Li, ''Proposed security mechanism for XMPP-based communications of ISO/IEC/IEEE 21451 sensor networks,'' IEEE Sensors J., vol. 15, no. 5, pp. 2577–2586, Mar. 2015.

[5] M. Dong, K. Ota, L. T. Yang, S. Chang, H. Zhu, and Z. Zhou, ''Mobile agent-based energy-aware and user-centric data collection in wireless sensor networks,'' Comput. Netw., vol. 74, pp. 58–70, Dec. 2014.

[6] R. Zhang, Y. Zhang, and K. Ren, ''Distributed privacy-preserving access control in sensor networks,'' IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1427–1438, Aug. 2012.

[7] L. Chen and J. Leneutre, ''A game theoretical framework on intrusion detection in heterogeneous networks,'' IEEE Trans. Inf. Forensics Security, vol. 4, no. 2, pp. 165–178, Jun. 2009.

[8] W. Lu, M. Tavallaee, and A. A. Ghorbani, ‘‘Detecting network anomalies using different wavelet basis functions,’’ in Proc. 6th Commun. Netw.Services Res. Conf., Halifax, NS, Canada, May 2008, pp. 149–156.

[9] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, S. Dubus, and A. Martin, ‘‘Success likelihood of ongoing attacks for intrusion detection and response systems,’’ in Proc. Int. Conf. Comput. Sci. Eng. (CSE), Vancouver, BC, Canada, Aug. 2009, pp. 83–91.

[10] H. Lee, K. Shin, and D. H. Lee, ‘‘PACPs: Practical access control protocols for wireless sensor networks,’’ IEEE Trans. Consum. Electron. vol. 58, no. 2, pp. 491–499, May 2012.

[11] M. Abdelhakim, L. E. Lightfoot, J. Ren, and T. Li, ‘‘Distributed detection in mobile access wireless sensor networks under Byzantine attacks,’’ IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 4, pp. 950–959, Apr. 2014.

[12] E. Y. Vasserman and N. Hopper, ‘‘Vampire attacks: Draining life from wireless ad hoc sensor networks,’’ IEEE Trans. Mobile Comput., vol. 12, no. 2, pp. 318–332, Feb. 2013.

[13] K. Q. Yan, S. C. Wang, and C. W. Liu, ‘‘A hybrid intrusion detection system of cluster-based wireless sensor networks,’’ in Proc. Int. MultiConf. Eng. Comput. Sci. (IMECS), Hong Kong, 2009, pp. 1–6.

[14] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, ‘‘Green firewall: An energy-efficient intrusion prevention mechanism in wireless sensor network,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), Anaheim, CA, USA, Dec. 2012, pp. 3037–3042.